

Conditions générales de vente d'EDS Media AG - Annexe A
Accord sur la protection des données conformément à l'EU-RGPD

Préambule

La présente annexe A (Accord sur la protection des données) des CGV (ci-après l'" Accord sur la protection des données ") définit concrètement les obligations des parties contractantes en matière de protection des données découlant du présent Accord sur la protection des données et du traitement commandé décrit à l'appendice A (Détails de la commande). Elle s'applique à toutes les activités liées au Service dans lesquelles les employés d'EDS ou les tiers mandatés par EDS peuvent entrer en contact avec les données personnelles de la clientèle (ci-après " le Client ") et/ou des clients du Client.

1. Définitions

Dans le présent accord de protection des données, les termes énumérés ci-dessous sont utilisés avec la signification suivante. Les autres termes sont définis dans les CGV.

Terme	Signification
Contrat	Contrat désigne le contrat de fourniture des Services conclu entre le Client et EDS sur la base des CGV d'EDS.
Responsable du traitement	Le responsable du traitement est la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou des États membres, le responsable du traitement ou les critères spécifiques de sa désignation peuvent être prévus par le droit de l'Union ou des États membres.
Personne concernée	La personne concernée est la personne physique identifiée ou identifiable à laquelle se rapportent les données à caractère personnel.
RGPD	RGPD désigne le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (règlement général sur la protection des données).
CGV	Les CGV font référence aux conditions générales de vente des EDS.
Instruction	L'instruction est l'ordre du client visant à un traitement spécifique de protection des données (par exemple, stockage, pseudonymisation, suppression, remise) des données personnelles par le EDS.
Ordre	Ordre désigne les services qu'EDS doit fournir à la demande du Client sur la base des CGV.
Traitement des ordres	Traitement commandé : les activités de traitement décrites à l'appendice A (détails de la commande), section 2.
Données à caractère personnel	Données à caractère personnel, toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »); est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, identité économique, culturelle ou sociale de cette personne physique.
Sous-traitant	Sous-traitant, la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

2. Champ d'application et responsabilité

- 2.1. L'EDS exécute le contrat. Dans ce contexte, le EDS obtient l'accès à des données personnelles et/ou peut prendre connaissance de ces données. Conformément à l'article 28 du RGPD, la conclusion du présent accord de protection des données est donc requise.
- 2.2. Le Client a sélectionné EDS en tant que prestataire de services dans le cadre des exigences de diligence raisonnable de l'article 28 du RGPD. L'admissibilité du traitement des données pour le compte du client est subordonnée à la condition que le client donne l'ordre à EDS par écrit ou sous forme électronique. Le présent accord de protection des données contient, selon la volonté des parties et en particulier du client, le mandat pour le traitement mandaté au sens de l'article 28, paragraphe 3, du RGPD et règle les droits et obligations des parties en matière de protection des données dans le cadre de la fourniture des services.

- 2.3. La propriété des données personnelles appartient exclusivement au client en tant que " responsable du traitement" au sens du RGPD. Sur la base de cette responsabilité, le client peut exiger la correction, l'effacement, le blocage et la remise des données personnelles pendant la durée de l'accord sur la protection des données et après la résiliation de l'accord sur la protection des données.

3. Objet et durée de l'ordre

- 3.1. L'objet de l'ordonnance figure à l'appendice A (détails de l'ordonnance).
- 3.2. Le présent accord entre en vigueur dès que le client a conclu le contrat et prend fin dès que les services concernés ont été fournis et que la période de conservation spécifiée à l'appendice A (détails du contrat) a expiré pour les données personnelles traitées pour permettre la fourniture des services. Le droit de résiliation extraordinaire du présent accord de protection des données n'est pas affecté.
- 3.3. En cas de doute, les dispositions du présent Accord de protection des données priment sur les dispositions du Contrat.

4. Description du traitement, des données et des personnes concernées

L'étendue et la finalité du traitement des données par EDS sont définies dans le contrat. Le type de traitement ainsi que le type de données et le groupe de personnes concernées sont décrits à l'appendice A (détails du contrat).

5. Mesures techniques et organisationnelles

- 5.1. EDS s'engage vis-à-vis du Client à respecter les mesures techniques et organisationnelles qui sont appropriées et nécessaires pour respecter les dispositions applicables en matière de protection des données.
- 5.2. EDS documente toutes les mesures techniques et organisationnelles qu'il prend et qui relèvent de l'article 28, paragraphe 3, point C, du RGPD, de l'article 32 du RGPD en liaison avec l'article 5, paragraphes 1 et 2, du RGPD et les remet au mandant pour examen si celui-ci en fait la demande par écrit.
- 5.3. Ces mesures servent à assurer la sécurité des données et à garantir un niveau de protection adapté au risque en matière de confidentialité, d'intégrité, de disponibilité et de résilience des systèmes associés à cette commande. L'état de l'art, les coûts de mise en œuvre et la nature, la portée et les finalités du traitement ainsi que la probabilité et la gravité variables du risque pour les droits et libertés des personnes physiques au sens de l'article 32, paragraphe 1, du RGPD sont pris en compte.
- 5.4. L'état des mesures techniques et organisationnelles existant au moment de la conclusion du contrat est joint en annexe B (Mesures techniques et organisationnelles pour la protection des données) au présent accord sur la protection des données. Les parties conviennent que des modifications des mesures techniques et organisationnelles peuvent s'avérer nécessaires afin de s'adapter aux circonstances techniques et juridiques. Le client peut demander à tout moment une version actualisée des mesures techniques et organisationnelles prises par EDS.

6. Correction, restriction et suppression des données

- 6.1. EDS ne peut pas corriger, supprimer ou restreindre le traitement des données personnelles qu'elle traite pour le compte du client de sa propre autorité, mais uniquement conformément aux instructions documentées du client. Si une personne concernée contacte directement EDS à cet égard, EDS transmettra immédiatement cette demande au client pour qu'il la libère.
- 6.2. La mise en œuvre des droits à l'effacement, à la restriction, à la rectification, à la portabilité des données et à l'information n'est assurée directement par EDS qu'en suivant les instructions documentées du client.
- 6.3. Aucune copie ou duplication des données ne doit être effectuée à l'insu du client. En sont exclues les copies de sécurité, dans la mesure où elles sont nécessaires pour assurer un traitement correct des données, ainsi que les données requises pour le respect des obligations légales de conservation.
- 6.4. Après la fin du contrat ou plus tôt sur demande du client - au plus tard toutefois à la résiliation de l'accord de protection des données - EDS détruira toutes les données personnelles du client qui sont entrées en sa possession et qui sont nécessaires à la fourniture des services conformément à la loi sur la protection des données. Il en va de même pour le matériel d'essai et de comité. L'enregistrement de la suppression est présenté sur demande.
- 6.5. EDS doit conserver la documentation qui sert de preuve du traitement ordonné et approprié des données conformément aux périodes de conservation respectives au-delà de la fin du contrat et/ou au-delà de la fin de l'accord de protection des données. Il peut les remettre au client pour qu'il les décharge à la fin de l'accord sur la protection des données.

7. Les fonctions de l'EDS

- 7.1. Il est interdit à EDS de traiter les données personnelles du Client qui ne sont pas liées à la fourniture des Services - sauf si le Client a consenti à un tel traitement par écrit.
- 7.2. En raison de son emplacement, de sa taille et des services qu'elle fournit, EDS n'est pas tenue de désigner un délégué à la protection des données conformément au RGPD. Cependant, EDS a décidé de nommer une personne responsable pour assurer la conformité au RGPD dans son entreprise. Ces coordonnées actuelles sont toujours disponibles et facilement accessibles sur le site web de l'EDS ou énumérées à l'appendice A (détails de la mission).
- 7.3. Le client est responsable de l'évaluation de l'admissibilité du traitement des données.
- 7.4. EDS informera immédiatement le client si, à son avis, une instruction donnée par le client viole les dispositions légales. EDS est en droit de suspendre l'exécution de l'instruction en question jusqu'à ce qu'elle soit confirmée ou modifiée par le client.
- 7.5. EDS informera le Client sans délai en cas de perturbations graves du processus opérationnel, de suspicion de violation de la protection des données ou d'autres irrégularités dans le traitement des données personnelles du Client.
- 7.6. Si EDS constate ou si des faits permettent de supposer que les données personnelles qu'elle traite pour le Mandant font l'objet d'une violation de la protection légale des données personnelles conformément à l'article 33 RGPD (violation de la protection des données ou incident de données), parce que, par exemple, elles ont été transmises de manière illicite ou que des tiers ont pris connaissance de ces données de manière illicite de quelque manière que ce soit, EDS informera le Mandant immédiatement et complètement par écrit ou sous forme de texte (fax/email) de la date, du type et de l'étendue du ou des incidents. La notification au client doit contenir au moins les informations suivantes :
 - Une description de la nature de la violation des données personnelles, y compris, dans la mesure du possible, les catégories et le nombre approximatif de personnes concernées, les catégories concernées et le nombre approximatif d'enregistrements de données personnelles concernés
 - Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact pour de plus amples informations
 - Une description des conséquences probables de la violation des données à caractère personnel
 - Une description des mesures prises ou proposées pour remédier à la violation des données à caractère personnel et, le cas échéant, des mesures prises pour atténuer les effets négatifs éventuels.

En outre, EDS est tenue d'informer sans délai le Client des mesures qu'elle a prises pour empêcher à l'avenir toute transmission illicite ou tout accès non autorisé par des tiers.

- 7.7. Sur demande, le EDS fournit au Mandant les informations requises pour le registre des activités de traitement conformément à l'article 30, paragraphe 1, du RGPD et, en tant que Processeur, tient lui-même un registre des activités de traitement conformément à l'article 30, paragraphe 2, du RGPD.
- 7.8. EDS veille à ce que les collaborateurs impliqués dans le traitement des données personnelles du Mandant soient tenus à la confidentialité conformément à l'article 28, paragraphe 3, phrase 2, lettre b, à l'article 29 et à l'article 32, paragraphe 4, du RGPD et aient été familiarisés au préalable avec les dispositions relatives à la protection des données qui les concernent. EDS et toute personne sous son autorité ayant accès aux données personnelles ne peuvent traiter ces données que conformément aux instructions du donneur d'ordre, y compris les pouvoirs accordés dans le présent accord de protection des données, sauf s'ils sont légalement obligés de traiter ces données. Cette obligation de confidentialité survit à la cessation de l'activité de traitement.
- 7.9. Le respect des obligations susmentionnées sera contrôlé par EDS ou par des tiers mandatés par EDS pour effectuer ce contrôle et sera prouvé de manière appropriée.
- 7.10. En outre, EDS s'engage à soutenir le Client conformément à l'article 28(3)(f) du RGPD dans le respect des obligations énoncées aux articles 34 à 36 du RGPD :
 - Dans le cadre de son devoir d'information des personnes concernées et du pouvoir adjudicateur dans ce contexte, de fournir sans délai toutes les informations pertinentes
 - Lors de la réalisation de l'analyse d'impact sur la protection des données
 - Dans le cadre d'une consultation préalable de l'autorité de surveillance
- 7.11. Le mandant et EDS coopèrent, sur demande, avec l'autorité de surveillance dans l'exercice de ses fonctions.
- 7.12. Dans la mesure où le Client fait l'objet d'un contrôle de la part de l'autorité de surveillance, d'une infraction administrative ou d'une procédure pénale, d'une action en responsabilité de la part d'une personne concernée ou d'un tiers ou de toute autre action en relation avec le traitement commandé par EDS, EDS soutiendra le Client au mieux de ses possibilités.

- 7.13. EDS contrôle régulièrement ses processus internes ainsi que les mesures techniques et organisationnelles pour s'assurer que le traitement des données dans son domaine de responsabilité est effectué conformément aux exigences du droit applicable en matière de protection des données et que la protection des droits de la personne concernée est garantie.

8. Droits et obligations du client

- 8.1. Les instructions du donneur d'ordre sont initialement déterminées par la présente convention de protection des données et peuvent être modifiées, complétées ou remplacées à tout moment par le donneur d'ordre par écrit ou sous forme de texte par des instructions individuelles. Le directeur d'école donne ses instructions par écrit ou sous forme de texte.
- 8.2. Toutes les instructions données doivent être documentées par le client et par EDS.
- 8.3. Le mandant doit informer immédiatement et intégralement EDS s'il découvre des erreurs ou des irrégularités concernant les dispositions relatives à la protection des données lors de l'examen des résultats de la commande.
- 8.4. Le mandant est responsable des obligations de notification résultant de l'article 33 paragraphe 1 RGPD.
- 8.5. Si le mandant donne des instructions individuelles qui dépassent le cadre convenu dans le présent accord sur la protection des données ou dans le contrat, les coûts liés à l'exécution de ces instructions sont à la charge du mandant.

9. La sauvegarde des droits de la personne concernée

- 9.1. Le mandant est responsable de la sauvegarde des droits de la personne concernée.
- 9.2. Dans la mesure où l'intervention d'EDS est requise pour la protection des droits des personnes concernées - en particulier le droit à l'information, à la correction, à la restriction, à la portabilité des données ou à la suppression - par le Mandant, EDS prendra les mesures respectives requises selon les instructions du Mandant.
- 9.3. Dans la mesure où une personne concernée s'adresse directement à EDS pour obtenir la rectification, l'effacement, la limitation ou la portabilité de ses données, EDS transmet sans délai cette demande au mandant.
- 9.4. Les dispositions relatives à une éventuelle rémunération des dépenses supplémentaires encourues par EDS en raison de services de coopération dans le cadre de l'affirmation des droits des personnes concernées vis-à-vis du Client ne sont pas affectées.

10. Pouvoirs de contrôle

- 10.1. Le mandant a le droit de contrôler une fois par an, dans la mesure nécessaire, le respect des dispositions légales en matière de protection des données, les mesures techniques et organisationnelles ainsi que le respect des instructions du mandant par EDS.
- 10.2. Le mandant peut procéder à ces vérifications soit directement, soit par l'intermédiaire d'un tiers neutre, à condition que ce tiers ne soit pas un concurrent.
- 10.3. Le Client doit donner à EDS un préavis écrit d'un mois avant l'inspection et doit fournir les coordonnées de la partie effectuant l'inspection. EDS peut refuser la partie désignée pour effectuer l'inspection pour des raisons justifiées. En cas de refus, les parties conviennent d'un commun accord de la désignation de la partie inspectante.
- 10.4. L'inspection peut être effectuée dans la mesure nécessaire pendant les heures d'ouverture normales respectives de l'EDS concerné, à condition que les processus opérationnels de l'EDS ne soient pas perturbés de manière disproportionnée par les inspections.
- 10.5. Le mandant doit documenter les résultats de l'inspection et en informer l'EDS sans délai. Si des circonstances sont identifiées lors de l'inspection qui doivent être évitées à l'avenir et nécessitent des modifications des processus de protection des données de l'EDS, le donneur d'ordre en informe l'EDS sans délai.
- 10.6. EDS fournit au Mandant toutes les informations demandées dans la mesure où elles sont nécessaires à l'exécution du contrôle au sens du paragraphe 1.
- 10.7. EDS fournit au Mandant les informations nécessaires si l'autorité de contrôle prend des mesures à l'égard du Mandant conformément à l'article 58 RGPD, notamment en ce qui concerne les obligations de notification et de contrôle.
- 10.8. EDS doit apporter la preuve de mesures techniques et organisationnelles qui ne concernent pas uniquement la commande spécifique, conformément aux spécifications de l'appendice A (détails de la commande). Ceci peut être fait par :
- Le respect des règles de conduite approuvées conformément à l'article 40 du RGPD.
 - La certification conformément à une procédure de certification approuvée en vertu de l'article 42 du RGPD

- Attestations, rapports ou extraits de rapports actuels émanant d'organismes indépendants (par exemple, auditeurs, contrôleurs, responsables de la protection des données, responsables de la sécurité informatique, contrôleurs de la protection des données).
- Certification appropriée par un audit de sécurité informatique ou de protection des données (par exemple, selon ISO 27001 ou Protection de base BSI)

10.9. Les coûts d'une inspection à l'EDS peuvent être facturés au mandant.

11. Relations de sous-traitance

- 1.1. Le Mandant accepte qu'EDS fasse appel à des sociétés externes pour l'exécution de ses services contractuels ou de services de sous-traitance. Une liste des sous-traitants actuellement utilisés figure à l'appendice A (section 3) du présent accord sur la protection des données.
- 1.2. EDS s'assure, soit directement, soit par le biais d'arrangements contractuels appropriés, que le sous-traitant secondaire est soigneusement sélectionné. Avant la mise en service, EDS vérifie que le sous-traitant ultérieur peut respecter les dispositions de l'accord de protection des données conclu entre le mandant et EDS. Il peut également charger un tiers de ce contrôle par le biais de dispositions contractuelles appropriées. En particulier, le EDS vérifie au préalable et régulièrement pendant la durée du contrat ou la durée du présent accord de protection des données, ou fait vérifier par un tiers sur la base d'arrangements contractuels appropriés, que le sous-traitant ultérieur a pris les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel conformément à l'article 28, paragraphe 3, point c), ainsi qu'à l'article 32 du RGPD en liaison avec l'article 5, paragraphes 1 et 2, du RGPD. Le EDS doit documenter le résultat de l'inspection et le fournir au client sur demande. Le EDS est tenu d'obtenir du sous-traitant ultérieur la confirmation qu'il a désigné un responsable interne de la protection des données au sens des articles 37 à 39 du RGPD.
- 1.3. EDS veille à ce que les dispositions convenues dans le présent contrat de protection des données et, le cas échéant, les instructions complémentaires du client s'appliquent également aux sous-traitants. EDS contrôle régulièrement le respect de ces obligations ou les fait contrôler par un tiers qu'elle charge de le faire sur la base de dispositions contractuelles appropriées.
- 1.4. Le sous-traitant ultérieur doit signer une déclaration d'engagement à cet effet. Le EDS doit fournir au client une copie de cette déclaration écrite d'engagement sur demande.
- 1.5. EDS est notamment tenue de s'assurer par des dispositions contractuelles que les pouvoirs de contrôle du donneur d'ordre et des autorités de contrôle s'appliquent également vis-à-vis du sous-traitant ultérieur et que les droits de contrôle correspondants sont convenus par le donneur d'ordre et les autorités de contrôle. Il doit également être réglementé contractuellement que le sous-traitant ultérieur doit tolérer ces mesures de contrôle et toute inspection sur place.
- 1.6. Si EDS traite des données personnelles en tout ou partie en dehors du territoire d'un État membre de l'Union européenne ou de l'Espace économique européen (EEE) ou d'un pays reconnu par l'Union européenne comme offrant un niveau de protection adéquat - y compris l'hébergement - EDS s'engage à encadrer le transfert des données personnelles par des garanties appropriées, y compris des clauses contractuelles types adoptées par la Commission européenne.

12. Obligations en matière de secret et de confidentialité des données

- 12.1. EDS s'engage à respecter les mêmes règles de protection des secrets que celles qui incombent au mandant. Le donneur d'ordre est tenu d'informer EDS de toute réglementation légale particulière en matière de protection des secrets.
- 12.2. Si le Donneur d'ordre en fait la demande par écrit ou sous forme de texte, EDS garantit qu'elle connaît les dispositions applicables en matière de protection des données et qu'elle est familiarisée avec leur application.
- 12.3. Les deux parties s'engagent à traiter toutes les informations reçues dans le cadre de l'exécution du présent accord de protection des données comme confidentielles pour une durée illimitée et à ne les utiliser que pour l'exécution des services. Aucune des parties n'a le droit d'utiliser ces informations, en tout ou en partie, à des fins autres que celles énoncées ci-dessus ou de les mettre à la disposition de tiers, sauf dans la mesure nécessaire à l'exécution du contrat, des sociétés affiliées du mandant ou d'EDS.
- 12.4. L'obligation qui précède ne s'applique pas aux informations que l'une des parties a manifestement reçues de tiers sans être tenue à la confidentialité ou qui sont connues du public.

13. Obligations du mandant

- 13.1. Le Client garantit qu'il a respecté toutes les lois et réglementations applicables en matière de protection des données et que lesdites lois et réglementations autorisent la divulgation des données personnelles à

EDS et leur traitement par EDS pour la fourniture des Services. Le Client garantit que tous les consentements nécessaires ont été obtenus des personnes dont les données doivent être traitées par EDS. Le Client s'engage à indemniser et à dégager EDS de toute responsabilité contre toute réclamation de tiers résultant de la violation de ces lois et règlements.

- 13.2. Le Client consent expressément au traitement, au stockage et à l'utilisation des données personnelles divulguées au sein du EDS afin que le EDS puisse remplir ses obligations contractuelles et légales, assurer une haute qualité de services et maintenir la relation client. Le Client s'engage à conclure sans délai des accords de protection des données plus spécifiques avec le EDS concerné si ce dernier en fait la demande par écrit ou sous forme de texte.

14. Devoirs d'information, clause de forme écrite, choix de la loi applicable

- 14.1. Si les données personnelles du Client sont menacées par une saisie, une procédure d'insolvabilité ou de concordat ou par d'autres événements ou mesures de tiers, EDS en informera immédiatement le Client. EDS informera immédiatement toutes les personnes responsables dans ce contexte que la souveraineté et la propriété des données personnelles appartiennent exclusivement au client en tant que " personne responsable " au sens du GDPR.
- 14.2. Les modifications et les compléments à cet accord de protection des données et à tous ses éléments - y compris les déclarations faites par EDS - nécessitent un accord écrit et l'indication expresse qu'il s'agit d'une modification ou d'un complément aux présentes conditions générales. Cela vaut également pour la dispense de cette exigence formelle.
- 14.3. Si une disposition du présent accord de protection des données est invalide, les autres dispositions restent néanmoins valables. Les parties contractantes s'engagent à remplacer de bonne foi une disposition invalide ou une disposition manquante involontairement dans la convention de protection des données par une disposition qui se rapproche le plus possible du but poursuivi en commun par les parties contractantes.

© EDS Media SA, août 2022

© EDS Media SA, inscrite au registre du 8706 Meilen, Suisse.

Appendice A: Détails de l'ordre

1. Objet de l'ordre

La commande passée par le client comprend les services rendus sur la base du contrat.

2. Portée, nature et finalité du traitement

L'étendue du traitement et donc la quantité de données personnelles sont variables et dépendent des services demandés par le client.

3. Informations sur l'organisation chargée de la protection des données (articles 28 et 32 de l'EU-RGPD)

Un délégué à la protection des données (DPO) a été nommé à l'EDS.

Nom et coordonnées de la personne de contact pour les questions relatives à la protection des données: Larissa Nöbauer / Téléphone +41 44 925 20 00 / E-mail : datenschutz@edsag.ch

4. Type de données et sous-traitants

Le type de données personnelles traitées dépend des services couverts par le contrat

Offres d'EDS	Données personnelles traitées	Durée de conservation	Personne ayant accès aux données personnelles
Business Mail	Prénom, nom de famille, fonction, adresse	Délai de livraison	EDS et/ou les sous-traitants chargés du processus de livraison (opérateurs postaux, transporteurs, partenaires)
Dédouanement	Prénom, nom, fonction, adresse, coordonnées douanières	Période de conservation légale (3 ans)	Sous-traitants mandatés par le service (partenaires locaux)
Direct Mail	Prénom, nom de famille, fonction, adresse	Délai de livraison	EDS et/ou les sous-traitants chargés du processus de livraison (opérateurs postaux, transporteurs, partenaires)
Marchandise	Prénom, nom de famille, fonction, adresse, adresse électronique, coordonnées douanières	Délai de livraison	EDS et/ou les sous-traitants chargés du processus de livraison (opérateurs postaux, transporteurs, partenaires) (opérateurs postaux, transporteurs, partenaires)
Presse	Prénom, nom de famille, fonction, adresse	Délai de livraison	EDS et/ou les sous-traitants chargés du processus de livraison (opérateurs postaux, transporteurs, partenaires) (opérateurs postaux, transporteurs, partenaires)
Courrier recommandé	Prénom, nom, fonction, adresse, numéro d'envoi	Durée du service + 6 mois de gestion après-vente	EDS et/ou les sous-traitants chargés du processus de livraison (opérateurs postaux, transporteurs, partenaires) (opérateurs postaux, transporteurs, partenaires)
Response Mail	Prénom, nom de famille, fonction, adresse	Durée du service	EDS et/ou les sous-traitants chargés du processus de livraison (opérateurs postaux, transporteurs, partenaires) (opérateurs postaux, transporteurs, partenaires)
Retouren	Prénom, nom, fonction, adresse, informations douanières sur les marchandises transportées	Durée du service + 6 mois pour la gestion après-vente	EDS et/ou les sous-traitants chargés du processus de livraison (opérateurs postaux, transporteurs, partenaires).
Suivi des envois	Vorname, Nachname, Funktionsbezeichnung, Adresse, Sendungsnummer	Prénom, nom, fonction, adresse, numéro d'envoi	EDS et/ou les sous-traitants chargés du processus de livraison (opérateurs postaux, transporteurs, partenaires).
Envois non livrables	Prénom, nom de famille, fonction, adresse	Durée du service	EDS et/ou les sous-traitants chargés du processus de livraison (opérateurs postaux, transporteurs, partenaires).

5. Catégories de personnes concernées

Les clients du mandant.

Appendice B: Mesures techniques et organisationnelles pour la protection des données

1. Confidentialité

1.1 Contrôle des entrées

Les personnes non autorisées doivent se voir refuser l'accès aux équipements techniques avec lesquels EDS fournit les services d'hébergement.

Mesures mises en œuvre à l'EDS :

- Système de verrouillage des bureaux et de la salle des serveurs
- Gestion des clés / documentation de l'attribution des clés
- Sélection minutieuse du personnel de nettoyage
- Règles obligatoires pour le traitement des visiteurs

1.2 Contrôle d'accès

Des mesures appropriées doivent être prises pour empêcher que les systèmes de traitement des données (matériel, systèmes d'exploitation, logiciels) soient utilisés par des personnes non autorisées.

Mesures mises en œuvre à l'EDS :

- Identifiant personnel et individuel de l'utilisateur lors de la connexion au système ou au réseau de l'entreprise
- Procédure de mot de passe (spécification des paramètres du mot de passe en ce qui concerne la complexité et l'intervalle de mise à jour)
- Verrouillage des clients après un certain temps sans activité de l'utilisateur (également économiseur d'écran protégé par mot de passe ou pause automatique)

1.3 Contrôle d'utilisation

Des mesures appropriées doivent être prises pour garantir que les personnes autorisées à utiliser un système de traitement des données ne puissent accéder qu'aux données faisant l'objet de leur autorisation d'accès et que les données à caractère personnel ne puissent être lues, copiées ou modifiées sans autorisation pendant leur traitement et leur utilisation ou après leur stockage.

Mesures mises en œuvre à l'EDS :

- Gestion des autorisations d'accès par les administrateurs du système
- Dans le but d'éviter les erreurs, une automatisation maximale lors de la mise en place des systèmes et des autorisations.
- Autorisations d'accès différenciées
- Concept de profil et de rôle

1.4 Contrôle du transfert

Des mesures appropriées doivent être prises pour que les données à caractère personnel ne puissent être lues, copiées, modifiées ou effacées sans autorisation lors de leur transmission électronique ou lors de leur transport ou de leur stockage sur des supports de données, et qu'il soit possible de vérifier et d'établir à quels moments, dans le cours normal des affaires, la transmission de données à caractère personnel est assurée par des équipements de transmission de données.

Mesures mises en œuvre à l'EDS :

- Connexions de données à distance par tunnel (VPN = Virtual Private Network)
- Transmission sécurisée des données sur Internet grâce au cryptage SSL (https)

1.5 Contrôle de la séparation

Des mesures appropriées doivent être prises pour garantir que les données collectées à des fins différentes puissent être traitées séparément.

Mesures mises en œuvre à l'EDS :

- Systèmes séparés (séparation logique des clients)
- Autorisations d'accès
- Séparation des systèmes de production et d'essai

1.6 Cryptage

Les données à caractère personnel sont traitées de manière à empêcher toute divulgation non intentionnelle, illégale ou non autorisée de ces données. Des mécanismes de cryptage de pointe, considérés comme sûrs, sont utilisés à cette fin.

Mesures mises en œuvre à l'EDS :

- Transmission de données cryptées (par exemple VPN, connexions internet cryptées SSL/TLS)

2. Intégrité

2.1 Contrôle de saisie

Il doit être possible de vérifier et d'établir rétrospectivement si et par qui des données à caractère personnel ont été introduites dans les systèmes de traitement des données, modifiées ou supprimées.

Mesures mises en œuvre à l'EDS :

- Privilèges d'accès
- Journalisation du système (journaux d'accès dans les différentes applications)

2.2 Commande de lecture

Les mesures de contrôle des transferts selon le point 1.4 servent également à garantir l'intégrité.

3. Disponibilité et résilience

Il convient de veiller à ce que les données à caractère personnel soient protégées contre toute destruction ou perte accidentelle.

Mesures mises en œuvre à l'EDS :

- Surveillance continue du serveur à l'aide d'un logiciel de surveillance
- Procédures de sauvegarde et d'archivage des données
- Protection contre les virus/pare-feu

4. D'autres domaines d'action

Une procédure doit être mise en œuvre pour l'examen, l'appréciation et l'évaluation réguliers de la protection des données et de l'efficacité des mesures techniques et organisationnelles définies.

Mesures mises en œuvre à l'EDS :

- Système de gestion de la sécurité de l'information (basé sur la norme ISO 27001)
- Système de réponse aux incidents pour la traçabilité des failles et des problèmes de sécurité
- Réalisation d'audits réguliers